# Cryptographic Module Validation Program

*International Topics*

Randall J. Easter

Director, NIST CMVP

September 14, 2004

# FIPS 140-2 to ISO/IEC…..

- FIPS 140-2 is the *de facto* international standard for cryptographic module security requirements
  - Cryptographic modules on the Validated Modules List developed by vendors from around the world
    - Australia, Israel, Singapore, U.K., France, Finland, Germany, Canada
  - Protection Profiles developed throughout the world reference FIPS 140-1 and FIPS 140-2
- FIPS 140-2 developed to facilitate conversion to an ISO standard

# ISO, *Security Requirements for Cryptographic Modules*

- Overview of changes
  - Inclusion of ISO terms and definitions
  - Inclusion of ISO references
  - Deletion of EMI/EMC section (a US FCC requirement)
  - Revisions based on proposed modifications to FIPS 140-2 (primarily “clean up”)
  - Revision of random number generator (RNG) tests to include ISO standards
    - Applicable to deterministic and non-deterministic RNGs